



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,351	12/11/2001	Howard G. Pinder	A-7274	8293

5642 7590 12/26/2006
SCIENTIFIC-ATLANTA, INC.
INTELLECTUAL PROPERTY DEPARTMENT
5030 SUGARLOAF PARKWAY
LAWRENCEVILLE, GA 30044

EXAMINER

NOBAHAR, ABDULHAKIM

ART UNIT	PAPER NUMBER
----------	--------------

2132

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	12/26/2006	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 12/26/2006.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOmail@sciatl.com

Office Action Summary

Application No.

10/015,351

Applicant(s)

PINDER ET AL.

Examiner

Abdulhakim Nobahar

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 October 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-124 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-124 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

Response to Arguments

1. This communication is in response to applicants' response received on August 01, 2006.
2. Applicant's arguments with respect to the rejections of claims 1-124 under 35 USC § 102 have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration of the amended claims, a new ground(s) of rejection is made.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-124 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rabowsky (6,141,530) in view of William Stallings, "Cryptography and Network Security, Principles and Practice", Second Edition, 1999 (hereinafter Stallings).

Regarding claims 1, 24, 38, 50, 55, 58, 69, 77, 83, 92, 100, 105, 110, 115 and 120, Rabowsky discloses:

Art Unit: 2132

receiving from a headend of the subscriber network a first ciphertext packet at the receiver (see, for example, col. 2, lines 27-46; col. 3, lines 33-35; col. 4, lines 21-32; col. 8, lines 51-62);

an input port adapted to receive a first key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has a single layer of encryption thereon that was applied by a first cryptographic algorithm using the first key (see, for example, Fig. 2; col. 4, lines 21-32; col. 8, lines 51-62; col. 10, lines 1-11);

a key generator adapted to generate a key (see, for example, col. 6, lines 52-56; col. 9, line 65-col. 10, line 10);

applying to the first plaintext packet a first cryptographic algorithm to convert the first plaintext packet to a ciphertext packet (see, for example, col. 4, lines 21-25; col. 11, lines 1-9);

a storage device in communication with the cryptographic device adapted to store the ciphertext packet and the keys (see, for example, col. 8, lines 51-62; col. 10, lines 12-25); and

a cryptographic device in communication with the input port and the key generator (see, for example, col. 9, lines 3-11; col. 9, lines 43-45; col. 9, line 65-col. 10, line 10).

Rabowsky, however, does not expressly disclose a scheme to use cryptographic algorithms to apply to the incoming encrypted packets from headend in order to convert them into ciphertext packets with three layers of encryption.

Stallings, on the other hand, discloses:

applying to the first ciphertext packet a first cryptographic algorithm to convert the first ciphertext packet to a second ciphertext packet (see, for example, page 94, Fig. 4.1(b), where at the encryption process, A is the incoming first ciphertext packet and undergoes an encryption operation to be converted to the second ciphertext packet B);

applying to the second ciphertext packet a second cryptographic algorithm to convert the second ciphertext packet to a third ciphertext packet (see, for example, page 94, Fig. 4.1(b), where at the encryption process, B is the second ciphertext packet and undergoes a second encryption operation to be converted to a third ciphertext packet C).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement the authentication scheme taught by Stallings in the system of Rabowsky to encrypt the incoming ciphertext packets two consecutive times to produce ciphertext packets with multiple layers of encryption because it would raise the cost of the known-plaintext attack (see Stallings, page 96, section "Triple DES with Two Keys").

Regarding claims 2, 15, 93, 94, 106 and 116, Rabowsky in view of Stallings discloses:

wherein the receiver is remote from the headend and located at a subscriber location; and further including the step of: storing the third ciphertext packet at the

Art Unit: 2132

subscriber location (see, for example, col. 1, lines 60-67; col. 8, lines 42-67).

Regarding claims 3, 40, and 84, Rabowsky in view of Stallings discloses:

wherein the third ciphertext packet is stored in a device external to the receiver (see, for example, Fig. 2, storage media 78).

Regarding claims 4, 7, 27, 36, 37, 39 and 85, Rabowsky in view of Stallings discloses:

wherein the third ciphertext packet is stored in an internal storage device of the receiver (see, for example, col. 10, lines 13-15).

Regarding claims 5, 35, 47 and 59, Stallings discloses:

wherein the third ciphertext packet corresponds to a cleartext packet that has been encrypted by a 3DES algorithm (see, for example, page 94, Fig. 4.1(b), encryption operation).

Regarding claims 6 and 97, Rabowsky in view of Stallings discloses:

wherein the first ciphertext packet includes encrypted content of a program distributed by the subscriber network (see, for example, col. 1, lines 467).

Regarding claims 7, 51, 61, 63, 70, 73, 75 and 78, Stallings discloses:

Art Unit: 2132

applying a third cryptographic algorithm to the third ciphertext packet to convert the third ciphertext packet to a cleartext packet (see, for example, page 94, Fig. 4.1(b), decryption operation).

Regarding claims 8, 53, 65, 90, 103, 108, 113, 118 and 123, Rabowsky in view of Stallings discloses:

converting the cleartext packet from a first format to a second format (see, for example, col. 2, lines 51-62; col. 3, line 9-15).

Regarding claims 9, 54, 66, 91, 104, 109, 114, 119 and 124, Rabowsky in view of Stallings discloses:

wherein the first format is an MPEG format (see, for example, col. 4, lines 6-10).

Regarding claims 10, 18, 23, 30, 49, 52, 57, 64, 74, 76, 87, 89, 96, 102, 112 and 122, Rabowsky in view of Stallings discloses:

wherein the third cryptographic algorithm is a 3DES algorithm (see, for example, col. 4, lines 20-32).

Regarding claims 11, 12, 31, 32, 33, 34, 43, 46, 60, 62, 71, 72, 79, 80, 86 and 98, Rabowsky in view of Stallings discloses:

Art Unit: 2132

wherein the first cryptographic algorithm is a DES algorithm (see, for example, col. 4, lines 20-32).

Regarding claims 13 and 25, Stallings discloses:

wherein the act of converting the first ciphertext packet to the second ciphertext packet removes a layer of encryption from the first ciphertext packet (see, for example, col. 6, lines 21-25; col. 6, lines 50-51; col. 12, line 64-col. 13, line 21, where using the first key of the 3DES keys for decryption of encrypted service instance corresponds to the recited removing a layer of encryption).

Regarding claims 14, 19 and 26, Stallings discloses:

wherein the act of converting the second ciphertext packet to the third ciphertext packet adds a layer of encryption to the second ciphertext packet (see, for example, page 98, section "Triple DES with Three Keys", where using a third key of the 3DES keys for encryption of already encrypted service instance with the 2nd key of the 3DES keys adds a layer of encryption to the ciphertext packet).

Regarding claims 15, 94 and 99, Rabowsky in view of Stallings discloses:

receiving a first key from the headend, wherein the first key is applied to the first ciphertext packet with the first cryptographic algorithm (see, for example, col. 10, lines 7-11).

Regarding claims 16, 28 and 68, Rabowsky in view of Stallings discloses:

generating an encryption key at the receiver, wherein the encryption key is applied to the second ciphertext packet with the second cryptographic algorithm (see, for example, col. 11, lines 47-53).

Regarding claims 17, 29, 67, 81, 82, 88, 95, 101, 107, 111, 117, and 121, Rabowsky in view of Stallings discloses:

receiving at least one key associated with the first ciphertext packet; and applying a third cryptographic algorithm with the at least one key and the encrypt key to convert the third ciphertext packet to a cleartext packet (see, for example, Rabowsky, col. 9, line 65-col. 10, line 10; Stallings, page 94, Fig. 4.1(b), decryption operation).

Regarding claims 20 and 41, Rabowsky in view of Stallings discloses:

generating at least one encryption key at the receiver, wherein the at least one encryption key is applied to the first ciphertext packet with the first cryptographic algorithm and the second ciphertext packet with the second cryptographic algorithm (see, for example, Rabowsky, col. 11, lines 47-53; Stallings, page 94, Fig. 4.1(b), encryption operation).

Regarding claims 21, 22, 41, 42, 44, 48 and 56, Rabowsky in view of Stallings discloses:

wherein the at least one encryption key is a first encryption key and a second encryption key, the first encryption key is applied to the first ciphertext

Art Unit: 2132

packet with the first cryptographic algorithm, and the second encryption key is applied to the second ciphertext packet with the second cryptographic algorithm (see, for example, Stallings, page 94, Fig. 4.1(b), encryption operation).

Regarding claim 45, Rabowsky in view of Stallings discloses:

wherein the cryptographic algorithm includes a first function and a second function, the first application of the cryptographic algorithm includes using the first function, and the second application of the cryptographic algorithm includes using the second function (see, for example, Stallings, page 94, Fig. 4.1(b), encryption operation, where the utilized DES algorithm has two functions; one for encrypting a clear service program and the other for decrypting the encrypted service program).

Conclusion

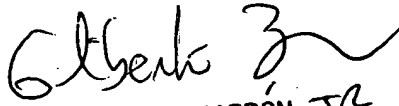
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

December 19, 2006

Abdulhakim Nobahar
Examiner, Art Unit 2132
GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100